

Amendments to the Claims:

This listing of the claims will replace all prior versions, and listings, of the claims in the application:

1 1. (Currently Amended) A computer-implemented method for creating an order-
2 invariant fuzzy commitment, comprising:
3 (a) receiving a first input element comprising a sequence of at least one value ($a_1, \dots,$
4 a_n) from a predetermined set;
5 (b) generating a codeword of an error-correcting code for generating the
6 commitment;
7 (c) constructing a first sequence of coordinate sets (x_i, y_i), for i in $\{1, \dots, n\}$, each of the
8 coordinate sets having a first value (x_i) corresponding to a representation of an associated
9 one (a_i) of the at least one value of the first input element and a second value (y_i)
10 corresponding to a symbol in the codeword, wherein the symbol corresponds to the x_i th
11 symbol in the codeword, wherein an order-invariant fuzzy commitment is formed, the
12 commitment having the property that it may be algorithmically combined with at least
13 one set of values comprising at least one value of the first input element so as to yield the
14 codeword; and
15 outputting the first sequence.

1 2. (Previously Presented) The method according to claim 1, wherein the
2 representation of the first value in the first sequence of coordinate sets is an integer
3 representation.

1 3. (Cancelled)

1 4. (Original) The method according to claim 1, further including deriving the first input
2 element from a measurement of a biometric associated with a user.

1 5. (Original) The method according to claim 4, further including selecting the biometric
2 from the group consisting of fingerprint information, retinal scan information, iris scan
3 information, bloodflow-pattern information, thermal imaging information, handwritten-

4 signature dynamics information, physiognomic information, hand geometry information,
5 and voice information.

1 6. (Original) The method according to claim 1, further including adding chaff to the
2 first sequence.

1 7. (Original) The method according to claim 6, further including adding the chaff as
2 sets of pairs of the form (x,y) such that x does not lie in the input sequence and y is
3 generated at random.

1 8. (Original) The method according to claim 6, further including adding the chaff as
2 sets of pairs of the form (x,y) such that one or more values x do lie in the input sequence
3 and y is generated at random.

1 9. (Original) The method according to claim 7, further including reordering the first
2 sequence based upon the first value.

1 10. (Original) The method according to claim 9, further including reordering the first
2 sequence in ascending order based upon the first value.

1 11. (Original) The method according to claim 1, further including applying a bijective
2 function to an input secret to obtain the codeword for the symbol corresponding to the
3 second value.

1 12. (Original) The method according to claim 1, further including decommitting the
2 order-invariant commitment by
3 receiving a second input element including a second sequence of at least one
4 value (b_1, \dots, b_m) from the predetermined set;
5 receiving the first sequence;
6 constructing a derived set of values ($X' = x_1', \dots, x_m'$) representing respectively
7 the at least one value (b_1, \dots, b_m) in the second sequence;

8 selecting a subset of the coordinate sets $\{(x_i, y_i)\}$ in the first sequence (E) such
9 that for each pair (x', y') in the subset, the first value in the pair (x') lies in the derived set
10 of values (X') ; and
11 applying an error-correcting function to the subset.

1 13. (Original) The method according to claim 12, wherein the error-correcting function
2 includes a Reed-Solomon code.

1 14. (Original) The method according to claim 1, further including selecting a polynomial
2 to generate the codeword.

1 15. (Original) The method according to claim 1, further including utilizing a decodable
2 design for decommitting the order-invariant commitment.

1 16. (Original) The method according to claim 1, further including utilizing a decodable
2 design comprising a design $D_{t,U,\Delta}$ and an algorithm M with running time polynomial in t
3 such that for any $S_i \in D_{t,U,\Delta}$ where $|S_i - S'| \leq \epsilon$, $M(S') = S_i$, U is a universe, t is a
4 cardinality of the design $D_{t,U,\Delta}$, Δ is a value less than t , such that $|S_i \cap S_j| \leq \Delta$, and the
5 design $D_{t,U,\Delta}$ includes a collection of sets $\{S_1, S_2, \dots, S_m\}$.

1 17. (Previously Presented) A computer-implemented method for decommitting an order-
2 invariant fuzzy commitment comprising:

3 receiving a first input element including a sequence of one or more values from a
4 predetermined set ;

5 receiving an order-invariant fuzzy commitment sequence;

6 constructing a set of integers having a predetermined number of elements
7 representing respectively values in the first input element;

8 selecting a subset of the coordinate sets in the first sequence such that the first
9 value in each subset coordinate set corresponds to the first value of at least one
10 coordinate set in the first sequence;

11 applying an error-correcting function to the subset; and

12 outputting the subset.

1 18. (Previously Presented) A computer-implemented method for creating a reordering-
2 tolerant fuzzy commitment comprising:

- 3 (a) receiving a first input element A including a first sequence of at least one value;
- 4 (b) generating a first codeword c of an error-correcting code for the commitment;
- 5 (c) constructing a sequence E of one or more data elements responsive to the first
6 input element A and the error-correcting code c ;
- 7 (d) outputting the sequence E ;
- 8 (e) receiving a second input element B including a second sequence of at least one
9 value and the sequence E , wherein the second sequence has a number of elements m ;
- 10 (f) applying a function d responsive to the second input element B and the sequence
11 E , wherein the function yields as output a value of a second codeword ($c' = d(B, E)$), the
12 function having a property such that $d(V, E) = c$ for at least one possible value of V , where
13 V comprises a third sequence having a number of elements m_V , wherein the at least one
14 value of the first sequence differs from the at least one value of the third sequence in at
15 least $m_V/2$ values; and
- 16 (g) outputting the second codeword c' .

1 19. (Previously Presented) A computer-implemented method for generating an order
2 invariant fuzzy commitment of an item of information, comprising:

- 3 receiving a first set of elements;
- 4 selecting a polynomial for encoding the item under the first set of elements to
5 generate an order-invariant fuzzy commitment of the item; and
- 6 storing said commitment in a computing device.

1 20. (Original) The method according to claim 19, further including inserting chaff points
2 that form a part of the commitment of the item.

1 21. (Original) The method according to claim 19, further including

- 2 receiving a second set of elements; and
- 3 selectively decommitting the item based upon a level of overlap of the first and
4 second sets of elements.

1 22. (Original) The method according to claim 21, further including determining the
2 polynomial from the second set of elements if the level of overlap is greater than a
3 predetermined threshold.

1 23. (Original) The method according to claim 21, further including utilizing an error-
2 correcting code for determining the polynomial.

1 24. (Original) The method according to claim 23, further including utilizing a Reed-
2 Solomon error detecting code.

1 25. (Original) The method according to claim 19, wherein the first set of elements
2 corresponds to a biometric template.

1 26. (Original) The method according to claim 19, further including utilizing a decodable
2 design to decommit the item, wherein the decodable design includes constituent pairs of
3 sets having a level of overlap less than a predetermined level.

1 27. (Original) The method according to claim 19, further including hiding the first set of
2 elements in a target set containing a plurality of elements selected from a field.

1 28. (Original) The method according to claim 27, further including projecting the first set
2 of elements onto the target set.

Claims 29-37 (Cancelled)

1 38. (Original) A computer readable medium, comprising code for enabling the steps of:
2 (a) receiving a first input element comprising a sequence of at least one value from a
3 predetermined set;
4 (b) generating a codeword of an error-correcting code; and
5 (c) constructing a first sequence of coordinate sets, each of the coordinate sets having
6 a first value corresponding to a representation of an associated one of the at least one
7 value of the first input element and a second value corresponding to a symbol in the
8 codeword, wherein the symbol is associated with the corresponding first value.

1 39. (Original) The computer readable medium according to claim 38, further including
2 code for enabling the steps of
3 receiving a second input element including a second sequence of at least one
4 value from the predetermined set;
5 receiving the order-invariant fuzzy commitment;
6 constructing a set of values representing respectively the values in the second
7 sequence;
8 selecting a subset of the coordinate sets in the first sequence such that the first
9 value in each subset coordinate set corresponds to the first value of at least one
10 coordinate set in the first sequence; and
11 applying an error-correcting function to the subset.

1 40. (Previously Presented) A computer-implemented method for creating an order-
2 invariant fuzzy commitment, comprising:
3 (a) receiving a first input element (A) comprising a sequence of at least one value
4 (a_1, \dots, a_n) from a predetermined set (F);
5 (b) generating a codeword (c) of an error-correcting code for generating the
6 commitment;
7 (c) constructing a first sequence (E) of coordinate sets (x_i, y_i) , for i in $\{1, \dots, k\}$ for
8 integer $k > 0$, each of the coordinate sets having a first value (x_i) corresponding to a
9 representation of an associated one (a_i) of the at least one value of the first input element
10 (A) and a second value (y_i) corresponding to a symbol in the codeword (c), wherein the

11 symbol is selected in a manner responsive to the first value x_i , wherein an order-invariant
12 fuzzy commitment is formed; and
13 outputting the first sequence.

1 41. (Previously Presented) A computer-implemented method for creating an order-
2 invariant fuzzy commitment, comprising:
3 (a) receiving a first input element (A) comprising a sequence of at least one value
4 (a_1, \dots, a_n) from a predetermined set (F);
5 (b) generating a codeword (c) of an error-correcting code for generating the
6 commitment;
7 (c) constructing a first sequence (E) of coordinate sets (x_i, z_i, y_i), for i in $\{1, \dots, k\}$ for
8 integer $k > 0$, each of the coordinate sets having a first value (x_i) corresponding to a
9 representation of an associated one (a_i) of the at least one value of the first input element
10 (A) and a second value (z_i) constructed in a manner responsive to a pattern of occurrence
11 of the associated one (a_i) of the at least one value of the first input element (A) in the
12 sequence (a_1, \dots, a_n) and a third value (y_i) corresponding to a subset of symbols in the
13 codeword (c), wherein the subset of symbols is selected in a manner responsive to at least
14 one of the first and second values of the coordinate set (x_i and z_i), wherein an order-
15 invariant fuzzy commitment is formed; and
16 (d) outputting the first sequence.

1 42. (Original) The method according to claim 41, further including decommitting the
2 order-invariant commitment by
3 receiving a second input element (B) including a second sequence of at least one
4 value (b_1, \dots, b_m) from the predetermined set (F);
5 receiving the first sequence (E);
6 constructing a derived set of values ($X' = x'_1, \dots, x'_m$) representing respectively
7 the at least one value (b_1, \dots, b_m) in the second sequence (B);
8 selecting a subset (E') of the coordinate sets $\{(x_i, y_i)\}$ in the first sequence (E)
9 such that for each pair (x', z', y') in the subset (E'), the first value in the pair (x') lies in
10 the derived set of values (X'); and
11 applying an error-correcting function to the subset (E').

1 43. (Previously Presented) A computer-implemented method for creating an order-
2 invariant fuzzy commitment, comprising:
3 (a) receiving a first input element (A) comprising a sequence of at least one value
4 (a_1, \dots, a_n) from a predetermined set;
5 (b) generating a codeword (c) of an error-correcting code for generating the
6 commitment;
7 (c) constructing a first sequence (E) of coordinate sets (x_i, z_i, y_i), for i in $\{1, \dots, k\}$ for
8 integer $k > 0$, each of the coordinate sets having a first value (x_i) corresponding to a
9 representation of an associated one (a_i) of the at least one value of the first input element
10 (A) and a second value (z_i) constructed in a manner responsive to information in the first
11 input element (A), and a third value (y_i) corresponding to a subset of symbols in the
12 codeword (c), wherein the subset of symbols is selected in a manner responsive to at least
13 one of the first and second values (x_i and z_i) of the coordinate set, wherein an order-
14 invariant fuzzy commitment is formed; and
15 (d) outputting the first sequence.

1 44. (Original) The method according to claim 43, further including decommitting the
2 order-invariant commitment by
3 receiving a second input element (B) including a second sequence of at least one
4 value (b_1, \dots, b_m) from the predetermined set (F);
5 receiving the first sequence (E);
6 constructing a derived set of values ($X' = x'_1, \dots, x'_m$) representing respectively the
7 at least one value (b_1, \dots, b_m) in the second sequence (B); and
8 selecting a subset (E') of the coordinate sets $\{(x_i, y_i)\}$ in the first sequence (E)
9 such that for each pair (x', z', y') in the subset (E'), the first value in the pair (x') lies in
10 the derived set of values (X'); and
11 applying an error-correcting function to the subset (E').

1 45. (Previously Presented) A computer-implemented method for creating an order-
2 invariant fuzzy commitment, comprising:
3 (a) receiving a first input element (A) comprising a sequence of at least one pair of
4 values $(a_1, w_1), (a_2, w_2), \dots, (a_n, w_n)$ wherein each of the at least one a_i values is from a first
5 predetermined set (F) and each of the at least one w_i values is from a second
6 predetermined set (G);
7 (b) generating a codeword (c) of an error-correcting code for generating the
8 commitment;
9 (c) constructing a first sequence (E) of coordinate sets (x_i, z_i, y_i) , for i in $\{1, \dots, k\}$ for
10 integer $k > 0$, each of the coordinate sets having a first value (x_i) corresponding to a
11 representation of an associated one $((a_i, w_i))$ of the at least one pair of values of the first
12 input element (A) and a second value (z_i) constructed in a manner responsive to an
13 associated one $((a_i, w_i))$ of the at least one value of the first input element (A) in the
14 sequence $(a_1, w_1), (a_2, w_2), \dots, (a_n, w_n)$ and a third value (y_i) corresponding to a subset of
15 symbols in the codeword (c), wherein the subset of symbols is selected in a manner
16 responsive to at least one of the first and second values of the coordinate set $(x_i$ and $z_i)$,
17 wherein an order-invariant fuzzy commitment is formed; and
18 outputting the first sequence.